White Paper

Access Protection in McAfee VirusScan Enterprise and Host Intrusion Prevention

Public release edition

Ben Andrew—MCSE

Senior Product Manager

McAfee® VirusScan® Enterprise (VSE) 8.7i, the leading enterprise-class anti-virus software solution, uses true on-access scanning to identify, proactively block, and safely eliminate viruses and potentially unwanted programs (PUPs) for optimal business availability. Centrally managed with McAfee ePolicy Orchestrator® (ePO™) and scalable for businesses of any size, VSE enhances the security of your company's computing systems by protecting them from programs that may be watching, recording, and externally transmitting sensitive company information.

Securing networks against a wide range of threats—viruses, spyware, worms, rootkits, and Trojans—is more challenging than ever. Whether you are a global enterprise or a small or medium-sized business that has a full-time security staff, VSE ensures that your endpoint servers, desktops, and laptops remain malware free. VSE proactively stops and removes threats, extends coverage for new security risks, and reduces the cost of managing outbreak responses. It even stops zero-day threats and mitigates your window of vulnerability without an update.

Access Protection in VirusScan Enterprise

A key component of VSE, Access Protection gives you flexibility to limit potential outbreak damage, even before a .DAT file is issued. You can also close ports, monitor applications and email engines, block files and directories, and trace and block infection sources.

Access Protection prevents unwanted changes to your computer by restricting access to specified ports, files and folders, shares, and registry keys and values. It prevents users from stopping McAfee processes and services, which are critical before and during outbreaks.

Access Protection for VSE uses predefined and user-defined rules to strengthen systems against virus attacks. For instance, rules are used to specify which items can and cannot be accessed. Each rule can be configured to block and/or report access violations when they occur, and rules can also be disabled.

The goal of this white paper is to provide an in-depth look at Access Protection and the importance and detail of the rules, which are organized into categories based on their function. The paper will explain the advantages and risks for Access Protection features, enabling you to determine which settings are optimal for your environment.

Extending Access Protection with McAfee Host Intrusion Prevention

The November 2008 content release for McAfee Host Intrusion Prevention (Host IPS) included new signatures that effectively duplicate the functionality of VSE's Access Protection rules. For greater control and flexibility, many customers have asked for the ability to manage these protections within Host IPS. The new signatures are disabled by default and set to log only in Host IPS to prevent accidental changes in your security posture and preferences. This white paper describes which Host IPS signatures map to VSE rules where applicable.

Access Protection Rules in VirusScan Enterprise

In the past, virus-scanning software depended primarily on the release of updated virus definition (.DAT) files that instructed the software how to detect and defend against new virus attacks. The use of .DAT files is still inherent in VSE; however, administrators now also have the ability to create rules that strengthen systems against further infection and provide a layer of intrusion prevention.

In VSE, all predefined rule definitions are stored in the file *vscan.bof*. This file is digitally signed and is updatable by the AutoUpdate process. The new rule-definition language used in *vscan.bof* allows a single rule to protect multiple objects of different types (file, registry, port, and process). The new rule language also allows inclusion and exclusion lists for the objects being protected. For example, a rule can block access to *c:*.exe* and *c:\temp*.exe* except for ***/notepad.exe*.

Purpose and application of rules

Rules should be created with one or more of the following purposes in mind:

- To prevent malicious code from running
- To identify which computers have malicious code running
- To prevent malicious code from spreading to other computers
- To prevent a payload from damaging the local computer

Rules can be created to target a specific, newly discovered threat, or they can be predefined to provide generic protection against future threats. For example, a rule might be used during the brief time between a virus outbreak and the release of a new .DAT file by McAfee Avert® Labs. During this time, it is important to stop the exploit from affecting the targeted systems and prevent it from spreading. In many cases, VSE can facilitate a new .DAT update and apply operating system patches without allowing the infection to spread. The rules are therefore not being used in place of virus definition files—they are used to compliment them.

Processing Access Protection rules

Access Protection rules can be located in two different files, as well as the registry, and rules can be processed in various ways based on the following conditions:

- *Vscan.bof* (located in the VirusScan directory) is the default Access Protection and buffer overflow protection content file. This file is read first.
- In an outbreak, Avert Labs may release an *extra.rul* before a new *vscan.bof* is available. If an *extra.rul* is present, (located in the VirusScan directory), it is appended.
- User-defined rules are read from the registry and appended.

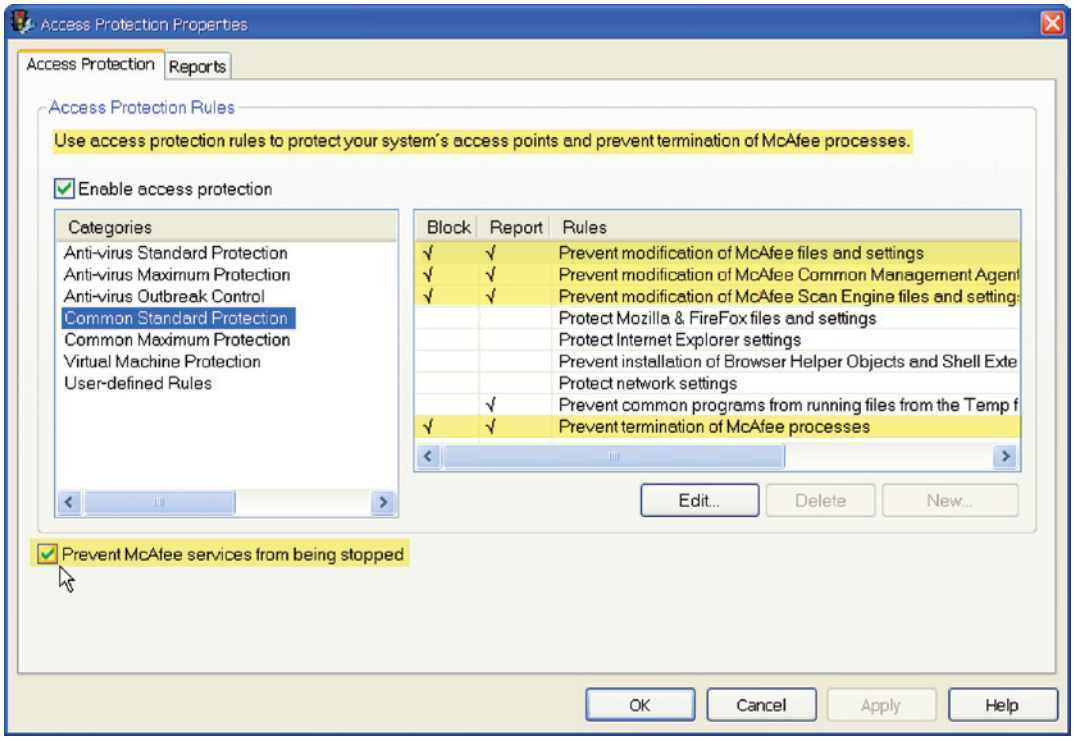
Self Protection

Many malicious programs have attempted to disable VirusScan by stopping services and processes and leaving the system vulnerable to attack. Self Protection is an important feature of VSE that prevents malicious programs from disabling VirusScan, or any of its services or processes.

"Prevent McAfee services from being stopped"

Self Protection begins with the check box in the lower left corner on the main Properties screen, and includes the following additional rules (listed throughout this document):

- Prevent modification of McAfee files and settings
- Prevent modification of McAfee Common Management Agent files and settings
- Prevent modification of McAfee Scan Engine files and settings
- Prevent termination of McAfee processes



Intention: When the **Prevent McAfee services from being stopped** check box is selected under Access Protection, VSE will prevent anyone except the SYSTEM account from terminating McAfee services. This protects VirusScan from being disabled by malicious programs that seek to circumvent virus protection programs by terminating their services.

Note: This feature is currently not supported on 64-bit operating systems.

Anti-spyware Standard Protection

This group of rules only applies if you have the AntiSpyware Enterprise Module installed. The rules for VSE begin in the section titled "Anti-virus Standard Protection."

"Protect Internet Explorer favorites and settings"

Intention: This rule is designed to prevent modification of Microsoft Internet Explorer configurations and files by any process not listed in the rule's exclusion list. A common tactic of malware is to change the browser's start page, and install favorites. This rule protects against certain start page Trojans, adware, and spyware that modify browser settings.

Risks: There really aren't any drawbacks to enabling this rule, as it simply blocks processes from making changes to favorites and settings in Microsoft Internet Explorer.

ID and Name in Host IPS:
3890, Access Protection—Protect Internet Explorer favorites and settings.

Anti-spyware Maximum Protection

"Prevent installation of new CLSIDs, APPIDs, and TYPELIBs"

Intention: This rule prevents the installation or registration of new COM servers. Some adware and spyware programs can install themselves as a COM add-on in Microsoft Internet Explorer or Microsoft Office applications.

Risks: If you have an application that needs to install a COM add-on that isn't already listed in the exclusion list, it will be blocked. The installation of some common applications, like Macromedia Flash, registers COM add-ons and may be blocked by this rule.

ID and Name in Host IPS:
3891, Access Protection—Prevent installation of new CLSIDs, APPIDs, and TYPELIBs.

"Prevent all programs from running files from the Temp folder"

This rule will block any executable from running from the Temp directory; however, this rule is much more restrictive in that it stops nearly all processes from launching in the Temp folder. This provides the most protection, but also has a higher chance of blocking a legitimate application from being installed.

Intention: Most viruses need to be run once by a person before infecting a computer. This can be done in many ways, such as opening an executable attachment in an email, downloading a program from the Internet, etc. For example, <http://vil.nai.com/vil/content/v_101034.htm>.

An executable needs to exist on the disk before Windows can run it. A common way for applications to achieve this is to save the file in the user's or system's Temp directory and then run it.

One purpose of this rule is to enforce advice that is frequently given to people: "don't open attachments from email." The other purpose of this rule is to close security holes introduced by application bugs. Older versions of Outlook and Internet Explorer are notorious for automatically executing code without the user needing to do anything but preview an email or view a website.

Risks: All applications that are protected by these rules offer alternatives to running executables, such as saving them somewhere else on the disk and running from there. So the downside of the rules is that users may need to learn a few extra steps before doing things they can do more quickly now.

Note: Enabling this rule may prevent some applications from functioning outright.

ID and Name in Host IPS:
3905, Access Protection—Prevent all programs from running files from the Temp folder.

"Prevent execution of scripts from the Temp folder"

Intention: This rule prevents the Windows scripting host from running VBScript and JavaScript scripts from the Temp directory. This would protect against a large number of Trojans and questionable web installation mechanisms that are used by many adware and spyware applications. This rule may also block legitimate third-party applications from being installed.

Risks: Since the email client downloads the script and then launches a legitimate Windows program (cscript or wscript) to process the script, this rule cannot distinguish between scripts that have been saved from a malicious email and those that have a legitimate reason for existing in the Temp directory. This rule may therefore prevent some legitimate scripts from running.

ID and Name in Host IPS:
3893, Access Protection—Prevent execution of scripts from the Temp folder.

Anti-virus Standard Protection

"Prevent Registry Editor and Task Manager from being disabled"

Intention: This rule protects some Windows registry entries to prevent the disabling of the registry editor and Task Manager. In the event of an infection, an administrator needs to have the ability to make changes to the registry, or open Task Manager to stop active processes.

Risk: Preventing the registry editor and Task Manager from running can make the manual removal of malicious code more difficult.

ID and Name in Host IPS:
3883, Access Protection—Prevent Registry Editor and Task Manager from being disabled.

"Prevent user rights policies from being altered"

Intention: Many worms attempt to locate accounts on network systems that have administrative rights. Enabling this rule prevents malicious code from modifying the rights of users. This rule protects registry values containing important Windows security information. For example, some viruses remove important privileges from the administrator account; this rule blocks those changes.

Included processes:	all
Excluded processes:	installers

ID and Name in Host IPS:
3884, Access Protection—Prevent user rights policies from being altered.

"Prevent remote creation/modification of executable and configuration files"

Enabling this rule will prevent other computers from making a connection and altering executables, files in the Windows directories, etc.

Intention: This rule forms a very cut-down version of the "make shares read-only" rule. First, the extension list is reduced to file types that viruses usually infect. Second, the blocked action is just "write," which prevents infection but also allows new files to be created. This protects against fast spreading worms or viruses, which traverse a network through open or administrative shares.

Risk: While there are reasons to copy executables around using Windows shares there are fewer, if any, reasons to modify executables on remote systems. This is usually indicative of attack behavior. These four rules are much less likely to false alarm than the broad "make shares read-only" rule but are also less secure.

ID and Name in Host IPS:
There is no corresponding signature in Host IPS.

"Prevent remote creation of autorun files"

Intention: Autorun files are used to automatically launch program files, typically setup files from CDs. Preventing other computers from making a connection and creating or altering *autorun.inf* files can prevent spyware and adware from being executed. There are a lot of spyware and virus programs distributed on CDs. Microsoft has disabled autorun in Windows XP Service Pack 2.

Included processes:	system:remote
Excluded processes:	none

ID and Name in Host IPS:
There is no corresponding signature in Host IPS.

"Prevent hijacking of .EXE and other executable extensions"

Intention: This rule protects the .EXE and other keys under HKEY_CLASSES_ROOT. Some viruses alter these keys to ensure that the virus is run when any other executable runs. Enabling this rule will prevent spyware and malware from modifying important operating system and executable files.

Included processes:	all
Excluded processes:	installers

ID and Name in Host IPS:

3887, Access Protection—Prevent hijacking of .EXE and other executable extensions.

"Prevent Windows Process spoofing"

Intention: Many viruses and Trojans run use the name of a Windows process. This rule prevents files from being created or executed with the most commonly spoofed names. The authentic Windows file is excluded.

Risks: None

Included processes:	all
Excluded processes:	none

ID and name in Host IPS:
3888, Access Protection—Prevent Windows Process spoofing.

"Prevent mass mailing worms from sending mail"

Intention: Many viruses and worms find email addresses on the infected system and send themselves to these addresses. They do this by connecting directly to the email servers whose names they have harvested from the local system. This rule prevents any process from talking to a foreign email server using SMTP. By blocking this communication, a machine may become infected with a new mass-mailing virus, but that virus will be unable to spread further by email. It prevents outbound access to SMTP ports 25 and 587 on all programs except known email clients listed as an exclusion.

Risks: Our list of exclusions cannot be complete—there are many third-party applications that send email. These will stop working until their process names are added to the list of exclusions. To add a process to the list of exclusions, highlight the rule, click Edit, and add the process name to the list of processes to exclude.

Included processes:	all
Excluded processes:	common browsers and email clients

ID, Name in Host IPS:
There is no corresponding signature in Host IPS.

"Prevent IRC communication"

Internet Relay Chat (IRC) is the preferred communication method used by botnet herders and remote-access Trojans to control botnets (a set of scripts or an independent program that connects to IRC). IRC allows an attacker to control infected machines that are sitting behind network address translation (NAT), and the bot can be configured to connect back to the command and control server listening on any port.

Intention: Many backdoor Trojans connect to IRC servers and receive commands from their authors. For example, *http://vil.nai.com/vil/content/v_98963.htm*. By blocking this communication, even if a system becomes infected with a new Trojan, it will be unable to communicate with the person or entity controlling it.

Risks: If IRC is used within a company, or if these ports are used for some other purpose, then the rule will block them until the processes using the ports are added to the exclusion list.

Included processes:	all
Excluded processes:	none
Blocked inbound ports:	TCP/UDP 6666-6669
Blocked outbound ports:	TCP/UDP 6666-6669

ID and name in Host IPS:
There is no corresponding signature in Host IPS.

"Prevent use of tftp.exe"

Trivial File Transfer Protocol (TFTP) provides basic file transfer with no user authentication. Many Trojans use TFTP because it is a rudimentary method to download additional code. Enabling this rule will prevent anything except Windows Update from using it to download other malicious code to the system.

Intention: Some viruses spread by exploiting buffer overflows in vulnerable applications. Code is injected into the process and then run. This code downloads the rest of the virus from the computer that just injected the download code. Often, the download code uses the Windows TFTP client (*tftp.exe*) to perform the download. Therefore, even if a system becomes infected with part of a new virus, it cannot become fully infected because it cannot download the rest of the code.

Risk: The most reported case where Windows needs access to *tftp.exe* is when installing a Windows service pack. When the service pack installer cannot upgrade *tftp.exe*, the install fails, it is generally advised to enable this rule, but disable it during the period when patches and service packs are being installed.

Included processes: all
Excluded processes: Windows Update

ID and name in Host IPS:
3889, Access Protection—Prevent use of tftp.exe.

Anti-virus Maximum Protection

Intention: Anti-virus Maximum Protection provides common rules that protect most critical settings and files from being modified. This level provides more protection, but may prevent the installation of legitimate software. If you cannot install software, we recommend that you disable Access Protection Maximum Protection first, and then enable it again after installation.

Risk: Maximum Protection rules should be used with caution as they can block common activities such as installation or execution of certain applications or processes. It is recommended that Maximum Protection rules be initially enabled for report only in order to determine if exclusions will be required.

"Prevent svchost executing non-Windows executables"

Intention: Svchost.exe is a system process belonging to the Microsoft Windows operating system, which handles processes executed from .DLLs. This program is important for the stable and secure running of your computer and should not be terminated. Because this is a key component of Windows, attackers attempt to use this process to register their own .DLLs that are not part of Windows. This rule makes *svchost.exe* only load Windows service .DLLs.

Included processes: svchost.exe
Excluded processes: none

ID and name in Host IPS:
3894, Access Protection—Prevent svchost executing non-Windows executables.

"Protect phonebook files from password and email address stealers"

Intention: This rule prevents malicious code from reading the list of the user's contacts, which are stored in *rasphone.pbk* files in the user's profile directories.

Included processes: all
Excluded processes: typical processes that access the address book

ID and name in Host IPS:
3895 (2), Access Protection—Protect phonebook files from password and email address stealers.

"Prevent alteration of all file extension registrations"

Intention: This is a stricter version of the "Anti-virus Standard Protection: Prevent hijacking of .EXE and other executable extensions" rule. Instead of just protecting .EXE, .BAT, etc., it protects all the extension options under HKEY_CLASSES_ROOT.

Systems running Microsoft Windows operating systems use a three- or four-letter identifier added to file names after a period (.) to identify a file type. When a file is opened, the file extension is used to decide what program should be used to open the file, or if the file is a program that should be run. Malware can modify the file extension registrations in such a way that execution of the malicious code is silent. This rule prevents malware from modifying the shell extension by modifying the shell extension for .TXT and executing every time you open a .TXT file. This rule prevents extension options by protecting the registry keys where the file extensions are registered.

Risks: If system administrators enable this rule, they will need to make sure to disable the rule when installing valid applications that will modify the file extension registrations in the registry.

Included processes: all
Excluded processes: explorer

ID and name in Host IPS:
3896, Access Protection—Prevent alteration of all file extension registrations.

"Protect cached files from password and email address stealers"

Intention: Some viruses look through the Internet Explorer cache for email addresses and website passwords. This rule prevents access to anything in the Internet Explorer cache except by Internet Explorer.

Risk: Any process that uses the WinInet library or hosts an Internet Explorer control in a window can access the cache; therefore, you may need to add process to this rule if it is enabled.

Included processes: all
Excluded processes: Internet Explorer; McAfee processes

ID and name in Host IPS:
3897, Access Protection—Protect cached files from password and email address stealers.

Anti-virus Outbreak Control

"Make all shares read-only"

Intention: Many viruses spread by copying themselves to open shares on the network or by infecting files on open shares, for example, *http://vil.nai.com/vil/content/v_99209.htm*. While shares can be protected by access control lists (ACLs), the ACL on the admin shares (C$, D$, Admin$, etc) cannot be edited and are read/write to administrators. If an administrator's system becomes infected, that infection can rapidly spread across a network. VSE's share blocking does not treat administrators differently–all write access is blocked. If there is a policy of making shares read only, this rule reinforces that policy by closing the administrative shares.

Risks: This is a very powerful rule. It is a good idea to assess the roles of the systems that will use this rule. In a typical environment, it is likely that this rule will be suitable for workstations and unsuitable for servers. The rule is intended to block viruses that will severely limit use of the computer or network, and it is only useful when computers are actively under attack. In addition to potentially affecting the day-to-day use of computers, these rules can also affect the way they are managed. If computers are managed by pushing files to them, this rule will prevent updates or patches from being installed. The management functions of McAfee ePO will not be affected if this rule is enabled.

ID and name in Host IPS:
There is no corresponding signature in Host IPS.

"Block read and write access to all shares"

Intention: This rule is intended for use when a share-hopping worm is known to be in the wild and actively spreading. In environments that prohibit file sharing, these rules can enforce that policy as it will prevent write access, or all access, from remote computers to the protected one.

Risks: This is a very powerful rule. System roles need to be assessed before the rule is enabled. In a typical environment, it is likely that this rule will be suitable for workstations and unsuitable for servers. It is intended to block viruses that will severely limit the use of the computer or network, and it is only useful when computers are actively under attack. In addition to potentially affecting the day-to-day use of computers, these rules can also affect the way that they are managed. If computers are managed by pushing files to them, this rule will prevent updates or patches from being installed.

ID and name in Host IPS:
There is no corresponding signature in Host IPS.

Common Standard Protection

The rules in this category are intended to block viruses, adware, spyware, etc., with rules that shouldn't need much modification.

"Prevent modification of McAfee files and settings"

Intention: Many viruses and Trojans attack anti-virus products. This rule, in addition to VSE's self-protection features, protects VirusScan registry values and processes from being altered or deleted by malicious code.

Risks: This rule protects the McAfee security product from modification by any process not listed in the policy's exclusion list. Many Trojans and viruses will attempt to terminate or even delete security products. If you use custom or third-party deployment and update tools to install or update VSE, add the process, which alters McAfee settings to the exclusion list. Not doing so may cause the installation or update to fail. It is recommended that you utilize McAfee ePO to deploy and update VSE.

Included processes:	all
Excluded processes:	Installers, McAfee processes

ID and name in Host IPS:
3898, Access Protection—Prevent modification of McAfee files and settings.

"Prevent modification of McAfee Agent files and settings"

Intention: This rule provides the same coverage as the above rule, except that it specifically protects the McAfee Agent that is deployed by McAfee ePO.

ID and name in Host IPS:
3899, Access Protection—Prevent modification of McAfee Agent files and settings.

"Prevent modification of McAfee Scan Engine files and settings"

Intention: Similar to the above two rules, this is another self-protection rule designed to protect the scanning engine against tampering.

ID and name in Host IPS:
3900, Access Protection—Prevent modification of McAfee Scan Engine files and settings.

"Protect Mozilla FireFox files and settings"

Intention: A common tactic of malware is to change the browser's start page, and install favorites. This rule is designed to prevent modification of Mozilla FireFox configurations and files by any process not listed in the rule's exclusion list. The rule protects against certain start-page Trojans, adware, and spyware which modify browser settings. There aren't any drawbacks to enabling this rule, as it simply blocks processes from making changes to favorites and settings in Mozilla Firefox browsers.

ID and name in Host IPS:
3901, Access Protection—Protect Mozilla FireFox files and settings.

"Protect Internet Explorer settings"

Intention: Similar to the previous rule, this is designed to prevent modification of Microsoft Internet Explorer settings by any process not listed in the rule's exclusion list. A common tactic of malware is to change the browser's start page. This rule protects against certain start-page Trojans, adware, and spyware, which modify browser settings. There really aren't any drawbacks to enabling this rule, as it simply blocks processes from making changes to settings in Microsoft Internet Explorer.

ID and name in Host IPS:
3902, Access Protection—Protect Internet Explorer settings.

"Prevent installation of Browser Helper Objects and shell extensions"

Intention: This rule prevents adware, spyware, and some Trojans that install as Browser Helper Objects from installing on to the host computer. This is an extremely popular method for adware and spyware installations. However, this rule could stop the legitimate installation of these objects.

Risks: If you have custom or third-party applications that need to install these objects, make sure that you've listed them in this rule's exclusion list. After installation, the rule can be re-enabled since this rule does not prevent installed Browser Helper Objects from working.

This rule, along with the rules above for Internet Explorer and FireFox, are more general purpose than some listed in the anti-virus and anti-spyware sections. They protect things like home pages, search pages, and toolbars in the Internet Explorer and Mozilla FireFox browsers, as well as preventing installation of Browser Helper Objects and other shell extensions.

ID and name in Host IPS:
3903, Access Protection—Prevent installation of Browser Helper Objects and Shell Extensions.

"Protect network settings"

Intention: Modifying network settings is a common tactic used to redirect traffic and transmit network activity or data. This rule protects a system's network settings from being modified by processes not listed in the exclusion list. It is designed to protect against Layered Service Providers that transmit data like your browsing behavior by capturing network traffic and sending it to third-party sites. Programs like Adware-CommonName and Adware-NDotNet fall into this Layered Service Provider category.

Risks: If you have legitimate processes that need to change the network settings, make sure that they are listed in the rule's exclusion list or disable the rule while changes are made.

Included processes:	all
Excluded processes:	Installers, Windows

ID and name in Host IPS:
3904, Access Protection—Protect network settings.

"Prevent common programs from running files from the Temp folder"

Intention: This rule prevents email attachments and executables from running on web pages. It is designed to block applications from installing software from the browser or from the email client, and it is effective in stopping email worms. It monitors your browser and email client and prevents them from running software from the Temp directory. This stops most adware, spyware, Trojans, and viruses that use executables in email or browser links to install. Well-behaved installers do not usually use the system Temp directory to hold installers; however, a custom or third-party application may be prevented from installing after this rule is enabled.

Risks: If you need to install an application that uses the Temp folder, make sure that installation process is listed in the exclusion list.

Included processes:	Common browsers and email clients
Excluded processes:	None

ID and name in Host IPS:
3905, Access Protection—Prevent all programs from running files from the Temp folder.

"Prevent termination of McAfee processes"

Intention: When the "Prevent termination of McAfee processes" rule is enabled, VSE will prevent any non-McAfee processes and those specifically excluded from terminating the process or service. This protects VirusScan processes from being disabled by malicious programs that seek to circumvent virus protection programs by killing their processes.

If this is set then no one (except excluded processes) can terminate a McAfee process using Task Manager, etc. ("Terminate" means forcing the process to end right now. The victim process has no say in the matter).

Risks: If this rule is enabled, manual methods to update .DAT files for VSE will not work. The recommended method of updating with the use of ePO tasks will continue to function with this rule enabled.

ID, Name in Host IPS:
There is no corresponding signature in Host IPS.

Common Maximum Protection

The rules in this category are intended to block viruses, adware, and spyware with much stricter rules that may be inappropriate for some computers and may need some customization before they can be enabled. These rules are often used temporarily or in extreme cases of lock down.

"Prevent programs registering to autorun"

Intention: Most adware, spyware, Trojans, and viruses attempt to register themselves in such a way that they get loaded every time the system is booted. This rule is designed to prevent any process not on the excluded list from registering processes that execute on every reboot.

Risks: Legitimate applications may also do this; these should be listed in the exclusions list or installed before this rule is enabled.

ID and name in Host IPS:
3906, Access Protection—Prevent programs registering to autorun.

"Prevent programs registering as a service"

Intention: This rule protects the registry keys and directories that viruses, spyware, etc., can use to load when a user logs on or when the computer restarts. It prevents the installation of any new service by processes not listed in the exclusions list. This is common practice with applications such as keyloggers, and Layered Service Providers like Adware-SAHAgent. This also provides some limited protection against installation of new kernel mode rootkits.

Risks: Enabling this rule may also block legitimate installations from registering themselves as services. It may also block installation of device drivers for new hardware. McAfee recommends that you either install that application prior to setting this rule to block or list the installation process in the exclusions list.

Included processes:	All
Excluded processes:	Installers, Windows update

ID and name in Host IPS:
3907, Access Protection—Prevent programs registering as a service.

"Prevent creation of new executable files in the Windows folder"

A common hiding tactic for adware, spyware, Trojans, and viruses, is to place their files in the Windows directory. You should add processes that have a legitimate need to place files in the Windows directory to the exclusions list. This rule will stop the addition of executable files to the Windows folder.

Intention: Viruses and Trojans often copy themselves to the Windows directory, hoping to hide among the list of files there with odd names. These rules prevent files being created by any process, not just from over the network. This rule prevents creation of .EXE and .DLL files in the Windows directory.

Risk: These rules will disable many software installers.

Included processes:	all
Excluded processes:	Installers, Windows update

ID and name in Host IPS:
3908, Access Protection—Prevent creation of new executable files in the Windows folder.

"Prevent creation of new executable files in the Program Files folder"

Intention: This rule prevents creation of .EXE and .DLL files from adware and spyware installing new executable files in the Program Files directory. It can stop new software installations if not launched from one of the excluded processes.

Risk: McAfee recommends that you either install applications prior to enabling this rule, or place the blocked processes in the exclusion list.

ID and name in Host IPS:
3909, Access Protection—Prevent creation of new executable files in the Program Files folder.

"Prevent launching of files from the Downloaded Program Files folder"

A common distribution method for adware and spyware is to have the user download an executable file and run it automatically from the Downloaded Program Files folder. This rule is specific to Microsoft Internet Explorer and prevents software installations through the web browser. It might also block the installation of legitimate software, so either install the application before enabling this rule or add the installation process to the exclusion list.

Intention: Internet Explorer runs code from the Downloaded Program Files directory, notably ActiveX controls. Some vulnerabilities in Internet Explorer and viruses place a .EXE file into this directory and run it. For example, *http://vil.nai.com/vil/content/v_101031.htm*. This rule closes that attack vector.

Risks: Downloaded Program Files is much more legitimate than Temp, so this rule can disable non-malicious applications. Two known programs disabled by this rule are Microsoft's transfer manager (*transfermgr.exe*) and the Apple QuickTime installer (*QuickTimeInstaller.exe*). You can permit these functions by adding them to the list of processes to exclude.

Included processes:	Internet Explorer
Excluded processes:	none

ID and name in Host IPS:
3910, Access Protection—Prevent launching of files from the Downloaded Program Files folder.

"Prevent FTP communication"

This rule is designed to block FTP (port 21) traffic from any process not listed in the exclusion list. FTP communication is frequently used by adware, spyware, Trojans, and viruses to receive or transmit data. It is also sometimes used by buffer overflow exploits to retrieve additional components. However, many third-party applications have a legitimate need to use FTP traffic, so they need to be listed in the exclusions list.

Intention: Viruses and Trojans may attempt to download malicious code, spyware may attempt to upload personal information, and adware may attempt to download advertisements. These rules prevent anything but the authorized processes from communicating via FTP.

Risks: FTP is a widely used protocol. If this rule is enabled on an FTP server, it will stop working until the server process is added to the exclusion list. While we have put popular FTP clients into the exclusions list, there may be many programs that could be added based on your particular environment.

Included processes:	all
Excluded processes:	common browsers, email clients and FTP clients

ID and name in Host IPS:
There is no corresponding signature in Host IPS.

"Prevent HTTP communication"

Many spyware, adware, and Trojan programs use port 80 for software downloads, bundled components, or updates. This rule will prevent any service (using *svchost.exe*) from communicating over port 80. This would stop common spyware and adware delivery mechanisms. Some server software uses port 80, although this isn't common in desktops.

This rule will block all HTTP communication for processes not in the exclusions list. Like FTP traffic, HTTP traffic is used by many applications to retrieve or transmit data. Spyware, adware, and Trojans also commonly use HTTP communication for software downloads of third-party components or updates. There are also many legitimate reasons for processes to communicate via HTTP. Many applications use a registration or self-update procedure that communicates over HTTP. Without the process being listed in the exclusions list, the traffic would be blocked; therefore, McAfee strongly recommends a thorough test and review cycle before enabling this rule.

Intention: Many Trojans download scripts or other Trojans from websites controlled by the Trojan's author. For example, *http://vil.nai.com/vil/content/v_100487.htm*. By blocking this communication, even if a system becomes infected with a new unknown Trojan it will be unable to download further malicious code.

Risks: HTTP is a very widely used protocol. While we have included popular web browsers in the exclusion list, there may be many programs you may need to add based on your particular environment.

ID and name in Host IPS:
There is no corresponding signature in Host IPS.

Virtual Machine Protection

The rules in this category are intended to block viruses, adware, spyware, etc., with strict rules that may be inappropriate for some computers, and may need some customization before they can be enabled. These rules are often used temporarily or in extreme cases of lock down.

"Prevent Termination of VMware Processes"

Intention: When the "Prevent termination of VMware processes " rule is enabled, VSE will prevent processes except VMware processes and those specifically excluded from terminating the process or service. This protects VMware processes from being disabled by malicious programs that seek to circumvent virus protection programs by killing their processes.

If this rule is set, no one (except excluded processes) can terminate a VMware process using Task Manager, etc. ("Terminate" means forcing the process to end right now. The victim process has no say in the matter).

Risks: There are no drawbacks to enabling this rule, as it simply prevents processes from terminating VMware processes or services.

"Prevent modification of VMware Workstation files and settings"

Intention: This rule protects VMware Workstation registry values and processes from alteration or deletion by malicious code.

Risks: This rule protects the VMware Workstation product from modification by any process not listed in the policy's exclusion list.

"Prevent modification of VMware Server files and settings"

Intention: This rule protects VMware Server registry values and processes from alteration or deletion by malicious code.

Risks: This rule protects the VMware Server product from modification by any process not listed in the policy's exclusion list.

"Prevent modification of VMware virtual machine files"

Intention: This rule protects VMware virtual machine files from alteration or deletion by malicious code.

Risks: This rule protects the VMware virtual machine files from modification by any process not listed in the policy's exclusion list.

User-defined Rules

There are three purposes a rule can have:

- Prevent malicious code running in the first place
- If malicious code is running, prevent it from spreading to other computers
- If malicious code is running, prevent a payload from damaging the local computer

And for each of those categories there are two sub-divisions:

- Target the rule at a known, newly discovered threat
- Target the rule at all unknown future threats of a particular type

In all cases we are assuming that the regular virus detection is unable to detect the code—probably because we are in the small window after the worm goes wild and before .DATs are released and distributed.

Targeting Rules at New, Known Threats

Introduction

The first reference for these will be the VIL entry for the newly discovered threat. For example, if *W32/Bagle.ab@MM* has just been discovered, then the VIL page *http://vil.nai.com/vil/content/v_125089.htm* will exist but the .DATs will not have been released yet.

The first priority will be to create one or more rules that prevent virus from infecting your computers. However, because the virus is known to be in the wild, you can assume that some of your computers are infected. Therefore, the second priority is to create rules that help identify those computers, and prevent the virus from spreading and causing damage.

Preventing infection

When the *W32/Bagle.ab@MM* virus runs, it copies itself to:

%windir%/system32/drvdll.exe
%windir%/system32/drvddll.exeopen
%windir%/system32/drvddll.exeopenopen
%windir%/CPLSTUB.EXE

Since Windows does not use these filenames, creating rules that prevent these files from being created should prevent the virus from infecting a machine with no side effects.

For example:

Process:	*
Wildcard:	%windir%/system32/drv*.exe
Prevent:	Create

Process:	*
Wildcard:	%windir%/cplstub.exe
Prevent:	Create

Similar rules will be sufficient for many new viruses.

The default rules that block creation of all executables in Windows directories may have side effects and might not be suitable for use in some environments.

In order of security

1. As many threats use random filenames, use the broad "prevent any executable from being created" rule all the time.
2. If that causes too many problems, use the broad "prevent any executable from being created" rule for the duration of the outbreak.
3. If even that causes problems, then use the virus-specific rules we derived above.

Preventing distribution and damage

If you suspect that a virus has already infected your computers, you need to identify which one and stop the virus spreading further.

Since this virus—*W32/Bagel.ab@MM*—has known filenames then using the "User Defined Detection" feature of VSE found in the "Unwanted Programs Policy" is a very good way of detecting the virus. The Access Protection rules can help as well.

If we change the above rules slightly to read:

Process:	*
Wildcard:	%windir%/system32/drv*.exe
Prevent:	Create, write, read, execute

Process:	*
Wildcard:	%windir%/cplstub.exe
Prevent:	Create, write, read, execute

The rules will trigger when a user logs on and the virus tries to run. This will also identify computers where the virus is already installed and prevent the virus from running again.

Again, rules of this form will be effective against many new viruses when they have known filenames.

The VIL article also says that *W32/Bagel.AB@MM* will mail itself using SMTP, it listens on port 2535 for instructions from its author and it downloads scripts from websites. All of this behavior can be blocked using the following port-blocking rules:

Port: 25
Direction: Outgoing
Exclusion list: Any SMTP clients that are allowed to run

Port: 2535
Direction: Incoming
Exclusion list: None

Port: 80
Direction: Outgoing
Exclusion list: Any web browsers that are allowed to run

The first and last of these are included by default in VSE. If they cannot be enabled all the time, enable them for the duration of the outbreak if possible.

The last thing that the virus does is "Files are created in folders that contain the phrase 'shar.'" There is a long list of filenames that the virus uses so it is not practical to make a separate rule for each file. A broader rule, which prevents any .EXE files being created in a directory that contains "shar" would look like:

Process: *
Wildcard: **/*shar*/**/*.exe
Prevent: create

The *W32/Bagel.ab@MM* virus doesn't contain a destructive payload. If we look instead at *W32/Shodi.c@MM* *http://vil.nai.com/vil/content/Print104469.htm*, the VIL says "it delivers a destructive payload, deleting … C:\NTDETECT.COM."

Therefore, a rule such as:

Process: *
Wildcard: c:\ntdetect.com
Prevent: delete

will prevent this virus from rendering the computer unbootable. Since ntdetect.com is a Windows file, preventing access to it may affect the application of Microsoft hot fixes or service packs.

Targeting Rules at Unknown Future Threats

Introduction

It is difficult to know how to combat unknown future threats. Very few viruses are innovative, so using historical information you can implement general, broad rules.

All of the VSE default rules, described below, are aimed at stopping new threats that behave like recent widespread threats.

The problem with broad rules that are aimed at preventing the general behavior of viruses is that they can block legitimate file access. Some of the problems include:

1) Blocking well-known ports can disable existing software. For example, VSE has rules, which selectively block ports 25 (SMTP), 20 and 21 (FTP), and 80 (HTTP).

   Well-known ports are used by many legitimate programs. Before applying the rule, run it in report mode for a while to verify that no programs need to use the ports that are blocked.

2) Blocking access to Windows files and directories prevents parts of Windows from functioning. For example, we have rules to prevent all access to *tftp.exe* or write access to Windows executables.

   The tftp rule can trigger as a false alarm when applications such as Explorer or Windows File Protection try to access files for read access.

   The write-prevention rules will block the installation of service packs and hot fixes.

3) Blocking access to Windows or Program Files files and directories.

   Doing this will block the installation of legitimate as well as malicious software.

Preventing infection

Rules to prevent infection can, in decreasing order of security:

- Stop the malicious code from getting to the system
- Allow it to get to the system but prevent it from being executed
- Allow it to get to the system and execute but prevent it from installing itself

For example, two common types of viruses are mass mailers and share-hoppers.

With mass mailers, there is nothing the Access Protection rules can do to prevent code from arriving on the computer, especially if it is buried within an email. However, using knowledge of how the email clients work, it is possible to prevent casual execution of the code.

With share-hoppers, it is possible to prevent the malicious files from arriving on the system by restricting incoming network connections from write access.

In both cases, if the code exists and runs, the first thing the virus does is ensure that it will continue to run. Once the virus is allowed to run, its options are much greater than when it is relying on the user, or other software, to launch it. It is therefore much harder to design good rules to stop it. One common thing that viruses do is copy themselves to the Windows directory and set some value in the registry to have the virus started on logon or when a particular application starts. The virus will run once and may do things other than installing itself, but after a reboot the virus should be disabled.

Preventing distribution and damage

As with the "Prevent installation" case above, the virus is already running and the aim of these rules is to slow or stop it spreading further, or to stop it from causing damage. Since the virus code is running, there is no limit to what it can try to do and it is impossible to write rules to stop everything. Again, we can look at what existing, successful viruses do and assume that the next one is going to try something similar. The rule to "Prevent mass-mailing worms from sending mail" is the best way to stop mass mailers from spreading themselves.

Viruses tend not to contain payloads designed to delete or corrupt the files on the computer they are running on. Instead, they are designed to stay hidden on the computer and attack other computers, for example by sending spam or participating in denial-of-service attacks. They can either be coded to do some particular task, to download and run code from somewhere else, or to receive orders directly from their masters.

Port blocking rules target these last two cases.

Of course, some viruses still do attempt to delete files. Critical files—either those that are needed to keep the computer running or those that contain irreplaceable data—can be protected with rules such as

Process: *
Wildcard: c:\Data\OrdersDatabase.db
Prevent: Delete

Port Blocking

Port blocking rules allow you to block incoming or outgoing traffic on specified ports and choose to log entries when attempts are made to access blocked ports. When you block a port, both Transmission Control Protocol (TCP) and the User Datagram Protocol (UDP) accesses are blocked. You can block ports by creating rules to specify which port numbers to block and whether to restrict access to inbound or outbound processes. You can also exclude processes from the rule if you want a specific process, or list of processes, to be allowed access to the otherwise blocked port. This can be very advantageous in an instance when a known virus accesses the system using specified ports. However, use caution as legitimate applications may also need to access the system on those same ports. To help counter a situation where a legitimate application needs access but protection is required for unknown applications, an exclusion list may be used.

Port blocking rules

To create user-defined port blocking rules, provide the following:

- Rule name—Type the name for this rule.
- Processes to include—Restrict access to the specified ports.
- Processes to exclude—Allow access to the specified ports.
- Starting port—Specify the first port number. This can be a single port or the starting number of a range of ports.
- Ending port—Specify the last port number in a range of ports.
- Inbound—Prevent systems on the network from accessing the specified ports.
- Outbound—Prevent local processes from accessing the specified ports on the network.

Note: If you block access to a port that is used by the ePolicy Orchestrator agent, or the McAfee Host Intrusion Prevention agent, the agent's processes are trusted and are allowed to communicate with the blocked port. All other traffic not related to these agent processes is blocked.

File/Folder Protection

File/Folder protection rules allow you to prevent read access, write access, file execution, and creation or deletion of files and folders. This feature can be very powerful in preventing intrusions, as well as stopping viruses from spreading during an outbreak. Once you restrict access to a file or folder, the restriction remains in place until the administrator removes it.

File/Folder protection rules

To create user-defined File/Folder protection rules, provide the following:

- Rule name—Type the name for this rule.
- Processes to include—Processes to include in this rule. Wildcards are allowed.
- Processes to exclude—Processes to exclude from this rule. Wildcards are allowed.
- File or folder name to block—Block access to the specified file or folder. Complete path to the folder, or file this rule will affect. Partial folder/file names with wildcards can protect multiple, similar folders/files with a single rule.
  Examples: C:\Folder, C:\Fol*, C:\Folder/*.exe
  - Browse file—Navigate to the file.
  - Browse folder—Navigate to the folder.
- File actions to prevent—Specify which action or actions you wish to block for the selected folder/file, with this rule; Read access, write access, file execution, file creation, file deletion, or any combination of these options.
  - Read access to files—Block read access to the specified files.
  - Write access to files—Block write access to the specified files.
  - Files being executed—Block files from being executed in the specified folder.
  - New files being created—Block new files from being created in the specified folder.
  - Files being deleted—Block files from being deleted from the specified folder.

Registry Blocking

Block users or processes from taking action on specified registry keys or values.

Registry-blocking protection rules prevent unauthorized programs from altering, creating, or deleting registry keys and values that they shouldn't.

Registry-blocking rules

To create user-defined registry-blocking rules, provide the following:

- Rule name—Specify the name for this rule.
- Processes to include—Restrict these processes from access. Wildcards are allowed.
- Processes to exclude—Allow access to these processes. Wildcards are allowed.
- Registry key or value to protect—Protect this registry key or value:
  - Select a root key or value from the drop-down list.
  - Type a key or value in the text box.

  Note: Selecting the root key or value from the drop-down list is optional. Use either of these methods to specify the key or value:
  - Select the root key or value from the drop-down list, then type the remaining path to the key or value in the text box.
  - Type the full path to the key or value in the text box.

- **Rule type—Select the type of rule:**
  - Key—This rule protects the specified key.
  - Value—this rule protects the specified value.
- **Registry actions to block—Select the actions you want the rule to block: read key/value, write key/value, create key/value, delete key/value, or any combination of actions.**
  - Read from key or value—Block reading from the specified key or value.
  - Write to key or value—Block writing to the specified key or value.
  - Create key or value—Block creating the specified key or value.
  - Delete key or value—Block deleting the specified key or value.

Summary

Access Protection, available in either McAfee VirusScan Enterprise or McAfee Host Intrusion Prevention, proactively stops and removes threats, extends coverage for new security risks, and reduces the cost of managing outbreak responses. Even without an update, it stops zero-day threats and mitigates your window of vulnerability.

Enabling Access Protection rules gives you the flexibility to limit potential outbreak damage, even before .DAT file is issued. You can also close ports, monitor applications and email engines, block files and directories, and trace and block infection sources.

Access Protection prevents unwanted changes to your computer by restricting access to specified ports, files and folders, shares, and registry keys and values. It also protects McAfee processes and services by preventing users from stopping them. This protection is critical before and during outbreaks.

McAfee, Inc.
3965 Freedom Circle
Santa Clara, CA 95054
888 847 8766
www.mcafee.com

5345wp_tops_vse-hips_access-protection_0109